

NATIONAL MARINE FISHERIES SERVICE POLICY DIRECTIVE 32-106

JUNE 16, 2003

Information Management

NOAA FISHERIES HEADQUARTERS NETWORK SERVER

DEPLOYMENT POLICY

NOTICE: This publication is available at: <http://www.nmfs.noaa.gov/directives/>.

OPR: F/CIO (B. Bradley)

Certified by: F/CIO (L. Tyminski)

Type of Issuance: Renewal (02/06)

SUMMARY OF REVISIONS:

NOAA Fisheries Headquarters Network Server Deployment Policy

Effective Date: 6/16/2003

Background

NOAA Fisheries Headquarters rejects over thirty thousands hostile probes of its network every week. Many of these probes are automated processes that search for vulnerabilities that can be exploited through a number of methodologies. In addition to these probes, there has been a marked increase in the proliferation of computer viruses that attempt to destroy a computer's operating system or create a denial of service attack, which can cripple network operations. These activities represent a great risk to the Agency's reputation, and its ability to perform its mission through increased on-line interaction with its constituents. These risks require that all systems deployed by NOAA Fisheries be properly maintained and protected from such attacks.

Issue

All servers, regardless of Operating System, require proper installation and configuration of software and services to ensure they do not present a security problem to themselves or other servers on the network. Proper operation also requires installation of all relevant security patches that are routinely issued by the manufacturer, regular backup of all critical system data and maintenance of the operating system. The addition of servers, especially those deployed by unqualified technical personnel, increases the likelihood that one of these critical activities may be overlooked.

In addition to configuration and maintenance issues, a one, or few, application per server deployment strategy may overwhelm the financial and human resources available to host applications or web pages. A wise use of existing resources, takes full advantage of these somewhat limited resources, and can result in substantial savings for a Program Office. The following policy and procedures for standardized deployment of Headquarters network server hardware will contribute to a decreased security risk, and a more efficient use of existing resources.

Policy

The Chief Information Officer (CIO) will approve the deployment of all network servers prior to their installation on the Fisheries Headquarters Local Area Network. This policy applies to all Headquarters organizations, and expressly excludes desktop personal computers used by a single user performing routine administrative functions, such as

word processing and electronic messaging. Systems deployed prior to this policy, may be reviewed for compliance, and are subject to the procedures outlined in this document.

Procedures

Through their Office Information Technology Coordinator (OITC), Program Offices wishing to deploy new server hardware at Fisheries Headquarters, regardless of Operating System, will submit a request to the Headquarters Infrastructure Team Leader, providing the following information:

- A. Purpose of the server deployment.
- B. Evaluation of why existing NMFS servers cannot be utilized.
- C. A project plan that addresses the following issues.
 - 1. Server manufacturer, model, hardware configuration and operating system.
 - 2. Proposed server location
 - 3. Designated server administrator responsible for the deployment, operation, maintenance and security of the server.
 - 4. Detailed description of intrusion prevention and detection capabilities, including security hardware and software (e.g., firewall and virus detection software); provisions for security training by the system administrator; procedures and schedule for operational processes, including monitoring, back-ups and disaster recovery; and inclusion of the proposed hardware into a current Headquarters' Local Area Network Disaster Recovery Plan.

The Infrastructure Team Leader will submit the information and project plan to the CIO with a recommendation for approval or disapproval.

The CIO and staff will work with the requestor to accommodate the request. If however the proposal is disapproved, the CIO staff will make every effort to ensure that an existing server is made available to fulfill the needs of the Program Office.

If approved, the Infrastructure Team Leader will work with the requesting office to ensure the server is properly deployed on the Headquarters' Local Area Network.

Server Deployment

Prior to deploying new hardware on to the Headquarters' production network, a meeting will be held to review the final server configuration and confirm the roles and responsibilities for maintaining the system.

The meeting will be chaired by the Deputy CIO, with the following participants:

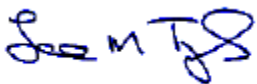
Infrastructure Team Leader
Software Development Team Leader
IT Security, Budget and User Services Team Leader
Information Technology Security Office
System Administrator
Program Office Contact / System Owner

The meeting participants will conduct a review of the system documentation, which will include at a minimum:

Server Configuration document
Updated Network Diagram
Standard Operating Procedures
System Configuration Change Request
Implementation Schedule

Upon review and approval by all meeting participants, the documentation will be forwarded to the CIO for final approval.

Signed,



Lawrence M. Tyminski
Chief Information Officer, NOAA Fisheries